

信息化网络安全管理和防范研究

奚永强

苏州江南航天机电工业有限公司 江苏 苏州 215100

摘要：信息化网络安全管理与防范是确保网络环境稳定和数据安全的关键，本文分析了信息化网络安全管理的重要性及现状，探讨了数据加密技术、网络存取控制、备份技术及防火墙技术等核心防范策略。提出了提升公众网络安全意识、完善管理制度、加强技术研发与应用等措施，通过这些措施，可构建坚固的网络安全防护体系，降低外部攻击风险，保障个人、企业及国家安全。

关键词：信息化；网络安全；管理；防范

引言

随着信息技术的飞速发展，网络安全问题日益严峻，成为制约信息化进程的一大障碍。个人隐私泄露、企业数据被盗、国家安全受威胁等事件频发，凸显了信息化网络安全管理的重要性。本文旨在深入探讨信息化网络安全管理和防范的现状与策略，为构建安全稳定的网络环境提供有益参考。

1 信息化网络安全管理的重要性

信息技术的飞速发展，互联网已成为现代社会不可或缺的基础设施，极大地促进了信息的流通与共享，为全球经济一体化和文化交流注入了强大动力，但是与之相伴的是日益严峻的网络安全问题，它已成为制约信息化进程的一大障碍。从个人层面来看，信息化网络安全管理直接关系到每个人的隐私保护和财产安全，数字化时代下的个人敏感数据多以电子形式存储和传输，一旦遭遇非法获取或滥用，个人隐私泄露、财产损失、身份盗用等严重后果将不期而至，所以利用加密技术、身份验证、访问控制等手段加强信息化网络安全管理，是维护公民基本权益的迫切需求。对于企业而言，信息化网络安全管理更是关乎其生存与发展的关键，企业核心资产一旦遭受网络攻击，将面临数据泄露、业务中断、声誉受损乃至生存威胁，有效的网络安全管理能构建坚固防御体系，及时发现并应对潜在威胁，确保企业运营稳定连续，同时提升客户信任度，增强市场竞争力。信息化网络安全管理在维护国家安全和社会稳定方面价值不可估量，网络空间作为国家主权的新疆域，网络安全已成为国家安全的重要组成部分，网络攻击、网络间谍活动、网络恐怖主义等新型安全威胁跨越国界，对国家安全构成重大挑战。加强信息化网络安全管理，构建国家层面的网络安全防护体系，是抵御外部威胁、维护国家主权和领土完整的重要手段，同时网络安全也是社会稳定的重要

保障，网络谣言、虚假信息、网络暴力等负面内容传播扰乱社会秩序，影响公众情绪，甚至激化社会矛盾，加强网络内容监管、提升公众网络安全意识，对于维护网络空间清朗和谐、促进社会稳定具有重要意义^[1]。

2 信息化网络安全管理现状分析

2.1 网络安全意识有待增长

一方面，信息化网络已深入人们日常生活，从在线购物、社交互动到远程办公、在线教育，极大地提升了生活便捷性和效率，渗透到社会各个角落；另一方面，公众在享受这些便利的同时，网络安全意识却显得滞后。许多用户在日常生活中往往忽视网络安全问题的关键性，不经意间进行高风险操作，如点击不明链接、使用弱密码或在不安全环境下传输敏感信息，这些行为极易成为不法分子攻击的突破口，导致个人隐私泄露、财产损失等严重后果。信息化网络的开放性虽然促进了信息共享和传播，但同时也埋下了安全隐患，黑客和不法分子可利用系统漏洞、恶意软件等手段窃取信息、破坏系统，甚至实施网络诈骗，对个人、国家安全、社会稳定及企业运营构成严重威胁。网络安全意识的薄弱还体现在对网络法律法规认知的缺失上，不少用户在无意中触犯法律红线，如传播谣言、侵犯隐私，面临法律制裁和社会舆论的双重谴责，所以提升公众网络安全意识需要政府、企业、学校及社会各界携手努力，通过宣传教育、培训讲座、法律法规普及等手段，增强公众对网络安全的认知和重视程度，并加强网络安全技术研发与应用，提升系统防御能力，及时修复安全漏洞，确保网络环境的安全稳定，有效保护自己的合法权益不受侵害。

2.2 病毒入侵

在信息化网络安全领域，计算机病毒构成了极其关键且严峻的挑战。这些由不法分子精心设计的恶意程序代码，通过自我复制或传播具有强大破坏力的形式，直

接针对服务系统核心发起攻击,旨在导致系统崩溃或严重功能障碍。计算机病毒以其多样且隐蔽的传播方式,如依附于网络文件、邮件附件、下载软件包或恶意网站链接中,在用户正常操作过程中悄无声息地潜入系统。一旦成功入侵,病毒便以惊人的速度和广度在网络内部迅速蔓延,利用系统漏洞或用户操作不当,跨越单个计算机乃至整个局域网,对整个网络环境造成广泛而深远的破坏。更难以应对的是,病毒设计之初便注重隐蔽性和抗杀毒性,能够巧妙隐藏、规避杀毒软件扫描,或通过变异对抗反病毒技术,使得彻底清除病毒成为一项耗时费力且往往难以完全成功的任务。在此期间,病毒可能已造成数据泄露、文件损坏、系统瘫痪等不可逆转的损害。尤其是,病毒能悄无声息地访问并复制个人隐私、企业商业秘密、政府机密等敏感数据,同时实时监控数据变化,为后续网络犯罪提供情报支持,对个人隐私、企业安全乃至国家安全构成双重威胁。而且计算机病毒的肆虐还破坏网络基础设施,影响网络服务的连续性和稳定性,导致企业业务中断、客户流失、声誉受损等连锁反应,极端情况下甚至可能引发社会恐慌和动荡,严重威胁国家安全和社会稳定。

2.3 网络安全管理制度建设不足

在信息化网络快速发展的时代背景下,网络安全管理工作正面临着前所未有的严峻挑战,其中,网络安全管理制度建设的滞后性和不完善性尤为突出,随着信息技术的持续进步,网络环境日益复杂多变,数据交换量急剧增长,这对网络安全管理提出了更为严格的要求。然而,当前许多组织在网络安全管理制度的建设上仍存在明显不足,这不仅体现在制度本身的缺失或过于笼统,更在于制度执行的不力和监督机制的缺乏。尽管越来越多的工作人员开始认识到网络安全的重要性,但在实际操作中,他们普遍缺乏足够的危机意识和主动防范意识,导致长效的安全管理机制难以建立。同时信息化网络结构中的海量数据内容使得系统运行维护工作变得异常复杂,工作人员在构建高效管理平台以确保数据安全性和可用性方面面临巨大挑战。由于技术、资金、人力等多方面的限制,许多组织在管理平台建设上难以取得预期效果,这不仅影响了数据的管理效率和质量,也制约了网络安全管理制度的有效实施。随着云计算、大数据、人工智能等新技术的不断涌现,信息化网络环境正经历深刻变革,但许多组织在网络安全管理制度的制定和执行上仍停留在传统模式,缺乏对新技术和新应用的深入理解和有效应对,这不仅限制了新技术在信息化网络建设中的应用和发展,也进一步加剧了网络安全管

理的风险和难度^[2]。

3 信息化网络安全管理和防范

3.1 数据加密技术

信息化网络安全管理和防范是维护网络环境稳定、保障数据安全的关键所在,随着网络技术的飞速发展,网络安全威胁日益多样化,给网络安全管理工作带来了前所未有的挑战,为了有效应对这些挑战,数据加密技术作为一项核心防护策略,发挥着举足轻重的作用。数据加密技术旨在确保网络数据在传输或存储过程中的保密性和完整性,防止数据被非法泄露或篡改。这一技术对于保护个人隐私、企业机密乃至国家安全具有极其重要的意义。数据加密技术主要包括检验加密和混合加密两种方式。检验加密通过复杂的加密算法和密钥管理机制,确保数据在传输过程中的完整性和保密性,有效防止数据被窃取或篡改。而混合加密则结合了多种加密技术的优点,通过多层次、多步骤的加密处理,进一步提升数据的安全性,为数据的传输和存储提供更加坚实的保障。但是仅凭数据加密技术并不足以全面保障网络安全,为了构建更加稳固的网络安全防线,我们还需要结合其他多种防护措施,这包括建立完善的网络安全管理制度和流程,加强网络设备和系统的安全配置与管理,定期进行安全漏洞扫描和风险评估,以及提升用户的网络安全意识和防范能力,通过这些综合措施的实施,我们可以更加有效地应对网络安全威胁,确保网络环境的稳定和数据的安全。

3.2 网络存取控制

网络存取控制作为维护网络安全、防止非法入侵及保护数据完整性的核心机制,其核心在于精确识别用户身份,确保网络资源与数据仅对合法用户开放。身份识别系统构成了网络存取控制的基础,通过要求用户在访问网络资源或服务时提供个人信息或特定密码来证明其访问权限,系统随后验证这些信息以判别用户的合法性。此过程中,确保身份识别信息的准确性和安全性至关重要,以防被非法用户利用或规避。为提高身份识别的准确性和安全性,数字签名技术被广泛采纳。数字签名是一种利用密码学原理对数据进行加密的电子签名,用于验证用户身份的真实性和数据的完整性。单体数字签名和双体数字签名是两种常见的数字签名方式。单体数字签名仅由签名者持有加密和解密密钥,因其保密性而具备高安全性;而双体数字签名则涉及签名者和验证者双方,通过公开签名者的相关信息供双方验证,增强了数据安全传输的灵活性。在实际操作中,网络存取控制还需结合其他安全措施,如建立访问控制列表

(ACL)限制用户访问权限、采用防火墙技术监控和过滤网络流量、定期进行安全审计和漏洞扫描,以全面提升网络存取控制的安全性和可靠性。

3.3 备份技术

备份技术在现代计算机系统管理中是确保数据安全、防范信息丢失不可或缺的一环,其重要性不仅体现在维护业务连续性上,更直接关联到企业的核心竞争力与客户信任,这一技术超越了简单的数据复制范畴,构建了一个包含数据存储、保护及恢复在内的全方位数据保护体系。在计算机系统的日常运营中,管理人员需定期且系统地对关键数据进行备份,既可选择在本机利用硬盘、U盘等本地存储设备确保数据的即时访问,也可通过网络云技术利用云计算的存储能力和高可用性实现远程备份与异地容灾,后者以其灵活性、可扩展性及成本效益显著降低了本地存储的硬件与维护成本。在实施备份策略时,“分散存储,安全保管”成为关键原则,即备份数据应远离主服务器,存放于独立且安全的空间,以防范主服务器故障、自然灾害或人为破坏导致的数据丢失,同时严格把控存放环境,确保防潮、防尘、防火、防盗及适宜温湿度,延长存储介质寿命,保障数据安全。加强对备份系统的有效维护同样重要,包括定期检查备份数据的完整性与可读性,及时更新备份软件与设备驱动程序以应对新威胁,以及制定并执行备份恢复演练计划,确保备份数据的可用性及恢复流程的可靠性。随着大数据、云计算等技术的飞速发展,备份技术也在不断革新,这些创新不仅提高了备份效率与准确性,还实现了在不干扰业务系统正常运行的前提下快速创建数据一致性状态副本,为数据的即时恢复提供了可能^[3]。

3.4 防火墙技术

防火墙技术是现代网络安全防护体系中的核心组成部分,扮演着网络第一道防线的关键角色,对于确保数据通信安全、阻止未经授权访问及抵御恶意攻击具有至关重要的作用,在实际部署中,防火墙技术的实施需紧密结合具体的工作需求和网络环境,通过精心配置网络中各设备的IP地址来保障通信的有序性。防火墙依据预设的安全策略和规则,对流经网络的信息进行深度过滤

与检查,这一过程不仅关注信息的来源与目的地,更重视深入分析信息内容特征,确保其符合组织的安全政策和业务需求。防火墙的核心功能在于其强大的信息过滤与访问控制能力,通过深度包检测(DPI)技术,防火墙能有效识别并拦截恶意软件、病毒、钓鱼攻击等潜在威胁,基于IP地址、端口号、协议类型等多种因素,制定精细的访问控制策略,允许合法必要的网络通信,阻止非法或不必要的访问请求,构建起一道坚固的安全屏障,显著降低外部攻击风险。在技术手段优化方面,防火墙的选择与应用需充分考量其特性与工作模式,各有优劣,需根据组织实际需求和网络架构选择最适合的类型与配置方案,并随着网络技术和攻击手段的演变,不断更新升级以适应新的安全威胁。加强对信息传输过程的全方位监督同样重要,包括实时监控网络流量、定期审计分析防火墙日志、建立应急响应机制等,以及时发现并响应异常行为,减少安全事件损失。同时防火墙技术还需与入侵检测系统(IDS)、入侵防御系统(IPS)、虚拟专用网络(VPN)技术以及身份认证和访问控制机制等安全技术和策略相结合,共同构建一个全面、高效、灵活的安全防护体系,进一步提升网络的安全性和可控性。

结语

综上所述,信息化网络安全管理和防范是一个复杂而系统的工程,需要政府、企业、个人等多方面的共同努力。通过提升公众网络安全意识、完善管理制度、加强技术研发与应用,我们可以构建更加坚固的网络安全防护体系,保障网络环境的安全稳定,为信息化建设提供有力保障。

参考文献

- [1]毛屹威.信息化网络安全管理和防范研究[J].数字技术与应用,2021,39(1):195-197.
- [2]贾潇辰.信息化网络安全管理和防范研究[J].缔客世界,2021(6):279-280.
- [3]鲁慧菊.信息化网络安全管理及防范对策研究[J].中国科技纵横,2023(15):74-76.